DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Risk Management and Incident Response
Incident Resolution Team

Monthly Report to Congress of Data Incidents

March 4 - 31, 2013

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000086343	Mishandled/ Misused Physical or Verbal Information	VISN 19 Sheridan, WY	3/4/2013	4/2/2013	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0586852	3/4/2013	INC000000266355	N/A	N/A	N/A		1

Incident Summary

On Sunday, 03/03/13 at 3:24 PM, Patient A checked in to the Sheridan VA Health Care System. At the time of check-in, Patient A received the document "Verification of Patient Demographic Data" for Patient B. Patient A went to his/her lodging place for the evening.

On Monday, 03/04/13 at 8:00 AM, Patient A reported back in for his/her appointments and told the clerk that he/she had received the "Verification of Patient Demographic Data" for Patient B the night before. The clerk took the form back and issued the Patient the correct paperwork.

Incident Update

03/04/13:
Due to full name, full SSN and date of birth being disclosed, Veteran B will be sent a letter offering credit protection services.

NOTE: There were a total of 121 Mis-Handling incidents this reporting period. Because of repetition, the other 120 are not included in this report, but are included in the "Mis-Handling Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

The responsible staff members were required to review check-in procedures and re-take the yearly privacy training.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000086355	Mishandled/ Misused Physical or Verbal Information	VISN 11 Ann Arbor, MI	3/4/2013	3/18/2013	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0586864	3/4/2013	INC000000266401	N/A	N/A	N/A		2

Incident Summary

Insulin medication was mailed to Patient A and Patient B. Patient A received Patient B's medication and Patient B received Patient A's medication.

Incident Update

03/04/13:
Patient A and B will be sent a notification letter.

NOTE: There were a total of 97 Mis-Mailed incidents this reporting period. Because of repetition, the other 96 are not included in this report, but are included in the "Mis-Mailed Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

The Pharmacy supervisor has advised the staff in regards to this incident report, and instructed them to double check the contents against the mailing label.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000086376	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Murfreesboro, TN	3/4/2013	3/19/2013	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0586878	3/4/2013	INC000000266476	N/A	No	N/A		1

Incident Summary

Patient A received a prescription intended for Patient B. Patient B's name and type of medication was compromised. Patient A reported the incident to the Medical Center and a replacement has been requested for Patient B. Murfreesboro Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a CMOP packing error. The CMOP employee(s) will be counseled and retrained in proper packing procedures.

Incident Update

03/05/13:
Patient B will be sent a notification letter.

NOTE: There were a total of 7 Mis-Mailed CMOP incidents out of 6,314,122 total packages (9,472,928 total prescriptions) mailed out for this reporting period. Because of repetition, the other 6 are not included in this report, but are included in the "Mis-Mailed CMOP Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter.

Resolution

The CMOP employee(s) was counseled and retrained in proper packing procedures.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000086759	Mishandled/ Misused Physical or Verbal Information	VISN 08 West Palm Beach, FL	3/13/2013		Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0587320	3/13/2013	INC000000268656	N/A	N/A	N/A	5	73

Incident Summary

Paperwork that was found in a public restroom in the facility included 3 pages with 55 names and partial SSNs and 1 page with 18 full names and partial SSNs, and 5 consults that contained full names, addresses, DOB and full SSNs.

Incident Update

03/14/13:
The documents also contained diagnosis information. The 5 patients whose DOB and full SSNs were on the papers will receive letters offering credit protection services. The other 73 will receive HIPAA letters of notification.

Resolution

The Health Tech submitted the information to the Privacy Officer (PO). The PO reported this incident to the Medical Administration Service (MAS) Supervisor to investigate and determine who left this information in the restroom.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000086861	Missing/Stolen Equipment	VISN 17 Dallas, TX	3/15/2013	3/22/2013	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0587428	3/15/2013	INC000000269303	N/A	N/A	N/A		

Incident Summary

Two obsolete laptops were unaccounted for during an IT Inventory.

Incident Update

03/18/13:
Two laptops were unaccounted for during a facility wide IT equipment inventory. The last known location for the first laptop was on the fifth floor in the clinical room 5B108 which is the GI Lab. It would have been a computer on wheels used for patients to sign I-Med consents. No personally identifiable information (PII) would have been on the laptop. All laptops were being encrypted prior to 2010, so the facility is confident this laptop was encrypted. The IT staff believe that this laptop was excessed after 2010 but cannot verify that. It's a Gateway model that was purchased in 2003.

The last known location for the second laptop was on the sixth floor of Building 2, Ward 6A. This was also a computer on wheels that was assigned to Nursing Service. No PII would have been on the laptop and it was encrypted. This laptop was purchased in 2008. The facility was excessing these models (HP Compaq 8510's) last year but cannot verify that this particular one was excessed. The computers on wheels are usually moved from ward to ward. The facility cannot discover it on the network.

NOTE: There were a total of 8 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 7 are not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Resolution

New OI&T Service Line is now in place with designated Inventory Control Specialist to enhance proper inventory control management.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000086896	Missing/Stolen Equipment	VISN 16 Alexandria, LA	3/18/2013		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0587465	3/18/2013	2013-USCERTv32OSBJ	N/A	N/A	N/A		

Incident Summary

A desktop computer has been reported as missing from a Conference Room. The computer was a Windows 7 system and was not encrypted. The desktop computer was mostly used for PowerPoint and did not contain any sensitive data on the system. The CPU, mouse, keyboard, network cables, power management system, and all power cords were removed. The computer was last signed onto at 3:13 AM on 03/15/13 by an employee; however, another employee reported not seeing the computer for morning reports later that morning. The computer was not reported missing to OIT Information Security Officer (ISO) until 9:14 AM on 03/18/13.

Incident Update

03/18/13:
According to the ISO, the PC did not contain any personally identifiable information (PII) or protected health information (PHI). The ISO confirmed with Police Service that a report was filed by OIT and the Administrative Officer (AO) of the Service. A copy of Police Report will be provided to ISO and Privacy Officer (PO) upon completion.

04/08/13:
There are no reports of the equipment showing up at the local pawn shops.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000087042	Mishandled/ Misused Physical or Verbal Information	VISN 18 Phoenix, AZ	3/21/2013		Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0587644	3/21/2013	INC000000270431	N/A	N/A	N/A	75	

Incident Summary

Today, 03/21/13, the Nurse Manager of Home Care reported a missing Veteran roster of the contract Community Based Nursing Home Veterans. A nurse who works in the community printed a paper list of approximately 75 Veterans for her community encounters on Wednesday, 03/13/13. The next day, the list was missing. Initial efforts to locate the list have included a search of her personal belongings, car and general call to the facility where the list was last seen. The list contained approximately 75 Veteran's first and last names, full SSNs, facility, diagnosis code, and specialty unit with notes.

The nurse agreed to do an additional search of belongings. Re-creation of the Veteran listing from 03/13/13 was requested. If the list is not found, immediate call to facility clinical POC with search methodology request there. Recovery efforts and results are pending. Privacy training records for 2 staff requested. Further investigation and notification is pending.

Incident Update

03/25/13:
Letters offering credit protection services will be sent to 75 Veterans.

Total number of Internal Un-encrypted E-mail Incidents	95
Total number of Mis-Handling Incidents	121
Total number of Mis-Mailed Incidents	97
Total number of Mis-Mailed CMOP Incidents	7
Total number of IT Equipment Inventory Incidents	8
Total number of Missing/Stolen PC Incidents	1
Total number of Missing/Stolen Laptop Incidents	6 (5 encrypted)
Total number of Lost BlackBerry Incidents	18
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	1